



UNITED STATES PATENT AND TRADEMARK OFFICE

mn
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,890	09/28/2001	E. David Neufeld	COMP:0224	4334

7590 05/16/2007
Intellectual Property Administration
Legal Dept., M/S35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER

TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
----------	--------------

2137

MAIL DATE	DELIVERY MODE
-----------	---------------

05/16/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 09/966,890	Applicant(s) NEUFELD ET AL.	
	Examiner Tamara Teslovich	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 2/20/07.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-6,9-11,13-19,22-27 and 29-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-6,9-11, 13-19, 22-27, 29-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 20, 2007 has been entered.

Claims 2, 7, 8, 12, 21 and 28 are cancelled.

Claims 1, 3-6, 9-11, 13-20, 22-27, and 29-40 are pending and herein considered.

Response to Arguments

Applicant's arguments and amendments, see pages 13-19, filed February 20, 2007, with respect to the rejection(s) of claim(s) 1, 3-6, 9-11, 13-20, 22-27, and 29-40 under 35 U.S.C. 101 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn.

Applicant's arguments with respect to the 35 USC 103 rejection of claims 1, 3-6, 9-11, 13-20, 22-27, and 29-40 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 27 and 29-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 27 recites the limitation "write the one or more bits to the seed pool" without explaining where said seed bits come from. The only mention of "seed bits" occurs a few lines previous wherein Applicant discloses "a non-volatile memory device to store a seed pool comprising a plurality of data bits." It is unclear whether or not the seed bits being written to the seed pool are those disclosed with respect to the already existing seed pool filled with already existing bits, or whether the bits being written are additional bits, and wherein those bits come from.

Claims 29-32 and 35 depend on claim 27 and are rejected accordingly.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 13-18, 27, 29-32 and 35 are rejected under 35 U.S.C. 102(b) as being anticipated by US Patent No. 5,680,131 to Utz et al., hereinafter referred to as *Utz*.

Regarding **claim 13**, Utz discloses a method of initializing a seed pool for generating a cryptographic key for a cryptographic security subsystem of a processor-based device, the method comprising the acts of (a) prior to enabling the cryptographic security subsystem, writing a plurality of bits of data to a seed pool (RS/PRNG), the plurality of bits of data having a signature (start) value (UTZ col.5 lines 34-42; col.6 lines 13-28); (b) detecting occurrences of a first type of triggering event and (c) writing one or more bits of data to the seed pool upon termination of the first type of triggering event, the one or more bits of data altering the signature value of the seed pool (col.6 lines 37-61); and (d) enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered (UTZ col.7 line 61 thru col.8 line 13; col.9 line 62 thru col.10 line 16); and generating a pseudo-random number from the seed pool, wherein the pseudo-random number is used to generate the cryptographic key for the cryptographic security subsystem of the processor based device (UTZ col.9 line 62 thru col.10 line 16).

Regarding **claims 14 and 15**, Utz discloses wherein the first type of triggering event comprises either a cycle of power applied to the processor-based device or a reboot of the processor-based device (power-on reset circuit) (UTZ col.5 lines 57-67).

Regarding **claim 16**, Utz discloses wherein act (c) comprises the act of masking (serially combining) the one or more bits of data into the seed pool (UTZ col.6 lines 57-61; col.5 line 22).

Regarding **claim 17**, Utz discloses wherein act (c) comprises the act of capturing the one or more bits of data from a free-running timer (clock signals) (UTZ col.5 lines 59-61).

Regarding **claim 18**, Utz discloses detecting a second type of triggering event; determining if the seed pool is full; and writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full (UTZ col.3 lines 38-40; col.11 lines 51-55).

Regarding **claim 27**, Utz discloses a processor-based device comprising: a host processing system, the host processing system comprising a processor and a communications management system in communication with the host processing system (UTZ col.5 lines 52-67); and a memory system in communication with the host processing system and the communications management system, wherein the communications management system comprises: an interface controller (UTZ col.6 lines 8-12); a non-volatile memory device to store a seed pool comprising a plurality of data bits (UTZ col.5 lines 34-42); and security logic in communication with the interface controller and the non-volatile memory device, the security logic configured to establish a secure communication session between the processor-based device and an external device in communication with the processor-based device via the interface controller (UTZ col.4 lines 47-60), and wherein the security logic is configured to: write the one or more bits to the seed pool, the bits altering a signature value; determine whether the plurality of data bits in the seed pool has at least a portion of a signature value; and

disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value (UTZ col.9 line 62 thru col.10 line 16).

Regarding **claim 29**, Utz discloses a main power supply to supply power to the processor-based device, and wherein the first type of triggering event comprises a cycle of the power supplied by the main power supply (power-on reset circuit) (UTZ col.5 lines 57-67).

Regarding **claims 30-31**, Utz discloses wherein the security logic is configured to detect a second type of triggering event; determine whether the seed pool is fully populated; and write one or more data bits to the seed pool upon termination of the second type of triggering event if the seed pool is not fully populated (UTZ col.3 lines 38-40; col.11 lines 51-55) and wherein the second type of triggering event comprises receipt of a communication from the external device via the interface controller (UTZ col.3 lines 38-40; col.11 lines 51-55).

Regarding **claim 32**, Utz discloses wherein the interface controller comprises a network interface controller (UTZ col.7 lines 41-45; col.10 lines 48-53).

Regarding **claim 35**, Utz discloses wherein the security logic is configured to detect a first type of triggering event, and to write one or more data bits to the seed pool upon termination of the first type of triggering event (UTZ col.6 lines 37-61).

Claims 36-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Bruce Schneier's "Applied Cryptography", hereinafter referred to as *Schneier*.

Regarding **claim 36**, Schneier discloses a method for restoring security data to non-volatile memory in a computer system comprising writing bits to a seed pool in discrete increments corresponding to a triggering event, wherein the seed pool is stored in a portion of a non-volatile memory device (pages 424, 426); tracking the state of the seed pool to determine if the seed pool is fully populated (page 426 "buflen"); and precluding access to the computer system if it is determined that the seed pool is not fully populated (page 428 lines 16-18).

Regarding **claim 37**, Schneier further discloses wherein the triggering even comprises receipt of a query from a device external to the computer system (page 426 lines 12-13).

Regarding **claim 38**, Schneier further discloses wherein writing bits to the seed pool in discrete increments corresponding to the triggering even comprises masking bits into the seed pool in discrete increments corresponding to a power cycle of the computer (page 426 lines 12-13).

Regarding **claim 39**, Schneier further discloses wherein tracking the state of the seed pool comprises examining a state bit, wherein the state bit changes when the seed pool is fully populated (page 426 "buflen").

Regarding **claim 40**, Schneier further discloses wherein tracking the state of the seed pool comprises examining the position of a pointer to determine whether the portion of the nonvolatile memory storing the seed pool is full (page 426 "buflen").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3-6, 9-11, 19, 22-26, 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier's "Applied Cryptography", hereinafter referred to as *Schneier*, and further in view of US Patent No. 5,680,131 to Utz et al., hereinafter referred to as *Utz*.

Regarding **claim 1**, Schneier discloses a method of generating a cryptographic key for a cryptographic security subsystem of a processor-based device, the method comprising the acts of (a) detecting occurrences of a first type of triggering event (SCHNEIER page 426 lines 6-14); (b) writing one or more bits of data to a seed pool (or reservoir) upon termination of the first type of triggering event, the seed pool comprising a state bit indicative of a state of the seed pool (SCHNEIER pages 424, 426, 427 "buflen"); (c) detecting occurrence of a second type of triggering event; (d) writing one or more bits of data to the seed pool upon termination of the second type of triggering event, wherein act (d) comprises masking one or more bits of data to the seed pool upon termination of the second type of triggering event (SCHNEIER page 426 lines 16-17); (e) examining the state bit to determine whether the seed pool is full (page 427

Art Unit: 2137

“buflen”); and (f) if the seed pool is not full, repeating acts (a) through (e) until (enough events have taken place) the seed pool is full (SCHNEIER page 428 lines 16-18); and generating a pseudo-random number from the seed pool, wherein the pseudo-random number is used to generate a cryptographic key for the cryptographic security subsystem of the processor based device (SCHNEIER pages 420-421).

Schneier fails to *specifically* mention masking bits into the seed pool.

Utz discloses the act of masking (serially combining) the one or more bits of data into the seed pool (UTZ col.6 lines 57-61; col.5 line 22) and writing one or more bits of data to the seed pool upon termination of the second type of triggering event (UTZ col.3 lines 38-40; col.11 lines 51-55).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Schneier the Utz’s ability to mask bits into the seed pool for use in creating a more random number.

Regarding **claim 3**, the combined system of Schneier and Utz teaches wherein the first type of triggering event has a variable duration (seemingly random events) (SCHNEIER page 426 lines 7-8).

Regarding **claims 4-6**, the combined system of Schneier and Utz teaches wherein that the processor-based device is coupled to a communication link, and includes the act of receiving a communication from the communication link (arrival times of network packets), the link comprising a plurality of types (network, multimedia, etc) (SCHNEIER page 426 lines 14-27).

Regarding **claim 9**, the combined system of Schneier and Utz teaches wherein that act (d) comprises capturing the one or more bits of data from a free-running timer upon termination of the second type of triggering event (SCHNEIER 426 lines 37-34).

Regarding **claim 10**, the combined system of Schneier and Utz teaches wherein the second type of triggering event is different than the first type of triggering event (as many good sources of randomness as are available) (SCHNEIER 426 lines 37-34).

Regarding **claim 11**, the combined system of Schneier and Utz teaches wherein the second type of triggering event is a cycle of power applied to the processor-based device (SCHNEIER page 426 lines 12-13).

Claim 19 is directed towards a device's implementation of the method of claim 1 and is rejected by similar rationale.

Claim 22 is directed towards a device's implementation of the method of claim 3 and is rejected by similar rationale.

Claim 23 is directed towards a device's implementation of the method of claim 4 and is rejected by similar rationale.

Claim 24 is directed towards a device's implementation of the method of claim 5 and is rejected by similar rationale.

Regarding **claim 25**, the combined system of Schneier and Utz teaches wherein the interface controller comprises an RS232 interface controller (UTZ col.7 lines 41-45; col.10 lines 48-53).

Claim 26 is directed towards a device's implementation of the method of claim 11 and is rejected by similar rationale.

Regarding **claim 33**, the combined system of Schneier and Utz teaches wherein the act of capturing one or more bits of data from a free-running timer (most finely grained time-of-day clock, for example the Intel 8254 clock chip) upon termination of the first type of triggering event (SCHNEIER page 426 lines 27-34).

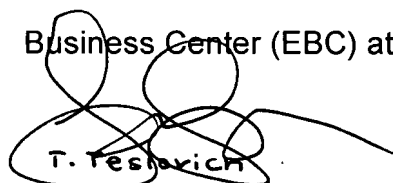
Claim 34 is directed towards a device's implementation of the method of claim 33 (cancelled claim 2) and is rejected by similar rationale.


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


T. Teslovich


MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137